Chapter 9

Electronic Warfare

9-1. General

a. Communications have always been the heart of command and control. On today's highly sophisticated battlefield, the Army places even greater dependence on communications and other battlefield electronic systems. The enemy knows this. A large part of the enemy's resources will be dedicated against U.S. Army command and control systems. Electronic Warfare (EW) will be used by both sides to an extent not known in the past. How vulnerable we are to enemy EW depends very much on the communicator.

b. TACSAT Company personnel must be trained to recognize the enemy's EW activities and to know what to do about them. This chapter introduces EW and highlights actions taken at the C-E operating level to minimize its effect. Specific tactics that will help defend against EW are found in FM 32–30 and equipment TMs.

9-2. Components of electronic warfare

Three components of EW are described in FM 32–30. They include all types of battlefield electronic systems: communications, surveillance, target acquisition, and others. This manual deals with EW only as it involves communications systems that support TA command and control. Table 9-1 summarizes the three components of EW as they pertain to communications devices. The first two EW components, electronic warfare support measures (ESM) and electronic countermeasures (ECM), are technical. We rely on military intelligence (MI) units and Intelligence and Security Command (INSCOM) for advice and implementation of ESM and ECM. The enemy equivalent of our ESM and ECM is described as radioelectronic combat (REC). To counter enemy use of REC, the Army relies on communicators to use electronic counter-countermeasures (ECCM).

9-3. Electronic threat

The enemy uses REC measures to collect intelligence data against our C-E systems. This is what intercept provides. The enemy then decides what REC would be appropriate from the data gained through intercept. High on enemy REC target list will be TACSAT communications. The enemy will use selected reconnaissance assets to detect and locate terminals, links, and relays. The enemy will attempt to those communications which he considers are priority targets. Figure 9-1 depicts the enemy's REC cycle. The goal of REC is to disrupt friendly use of the electromagnetic spectrum through destruction, deception, or jamming. The enemy will coordinate all three in an attempt to deprive us of command and control. All TACSAT Company personnel must understand the severity of this electronic threat.

a. Interception of signals intelligence. It is difficult for the enemy to fix on a satellite terminal. However, the radios used for TACSAT Company command and

Table 9-1. Components of electronic warfare

Component	Objective	Actions
ESM	Disclose information about enemy communications	Search, intercept, identify, locate
ECM	Deny or reduce use of enemy communications	Jam, deceive
ECCM	Ensure continued effective use of friendly communications (protect against enemy detection, location, and identification)	Anti-jam, circuit discipline, use approved operating techniques, security, harden, move, improve equipment, report, plan, train

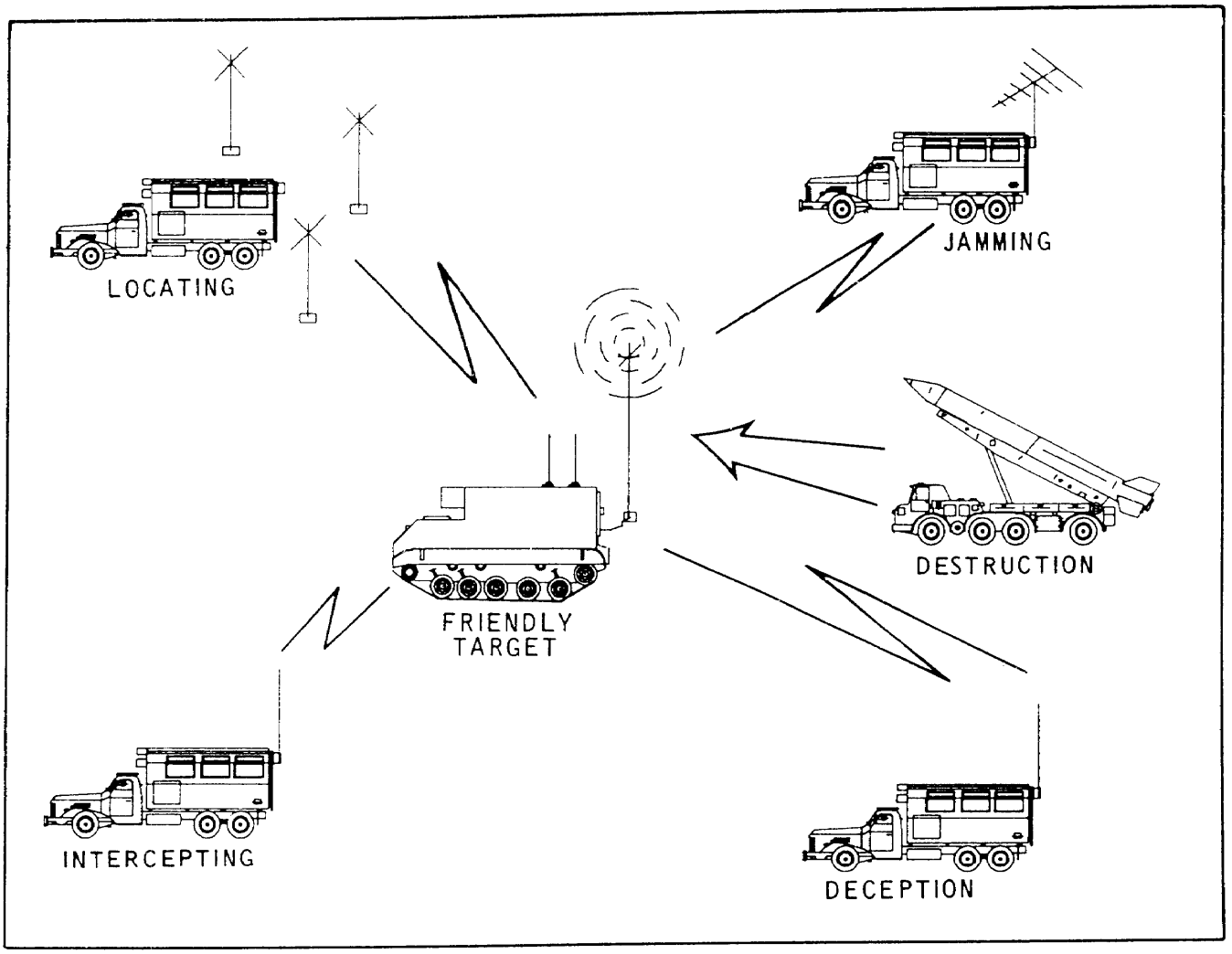

Figure 9-1. Enemy radioelectronic combat (REC) cycle

control are highly vulnerable to REC. Through an alert enemy signals intelligence effort, the Army risks disclosing Army TACSAT capabilities and operations. The enemy monitors intercepted signals and performs traffic analysis to provide a variety of information which can be exploited, such as—

(1) Supported CP identification.
(2) Location of TACSAT terminals.
(3) Tracking of unit movements.
(4) Relative importance of TACSAT to command and control.
(5) Weaknesses in our command and control systems—poor operating procedures, poor COMSEC, lack of redundant or alternate systems, and overloaded networks.

b. Location of emitters. A primary REC threat is the enemy's ability to locate key communications through radio direction finding (RDF). The enemy's goal is to limit, delay, or nullify our command, control, and intelligence systems during critical combat periods. RDF is especially effective against CPs which rely heavily on radios with omnidirectional antennas. Through the RDF technique, the TACSAT terminals themselves may be placed in jeopardy. When the enemy locates a friendly communication emitter, he determines if it is a primary target. Once an emitter becomes a primary target, disruption may take the form of destruction, deception, or jamming.

(1) *Jamming.* Enemy jammers attempt to disrupt the Army's conduct of the battle by interjecting delay and confusion into the command and control communications system. These jammers operate against receivers, not transmitters. They attempt to

transmit with enough power to override friendly signals before they can be received. This jamming may be subtle and difficult to detect, or it may be overt and obvious. It can be accomplished from both ground and aerial platforms. However jamming is accomplished, it is often most effective when opertors become impatient and relax signal security (SIGSEC) and OPSEC procedures, thus providing additional opportunities for deception or destruction operations. TACSAT radio operators must be familiar with this form of EW. The more common jamming signals are described in FM 32-30.

(2) *Deception.* REC attempts to deceive friendly emitters through intercepting, locating, and inserting false or misleading information. Enemy REC may imitate friendly forces to gain access to Army communications nets or provide incorrect or misleading information over enemy communications links. They may also establish dummy nets to feed false information to Army forces or to simulate nonexistent forces.

9–4. Defensive electronic warfare

Communications can still operate within the REC environment just described. To do this, it is necessary to maximize the efficiency of available equipment and use sound, common sense countermeasures. Communications discipline, security, and resourcefulness underlie countermeasures to shield emissions. COMSEC techniques give the commander confidence in the security of communications materials and communications. ECCM techniques provide some degree of confidence in the continued use of communications in a hostile EW environment. The two are closely related; many COMSEC techniques also serve an ECCM role. Thus, the more effective the TACSAT Company is in COMSEC, the more effective it is in ECCM.

a. Communications security techniques.

(1) COMSEC is a component of SIGSEC. It protects communications through the use of security measures and techniques such as those shown in table 9-2.

(a). Physical security safeguards COMSEC materiel and information from access or observation by unauthorized personnel through the use of physical means.

(b). Crypto security protects radio communications through the use of technically sound cryptosystems.

(c) Transmission security is designed to protect transmissions from hostile intercept and exploitation.

(d) Emission security involves studies, investigations, and tests to control comprising and inadvertent emissions from equipment.

(2) Most TCS(A) circuits are protected by COMSEC equipment. However, orderwire and internal TACSAT Company command and control nets may not be secure. Technical discussions between operators can contain information of vital importance to the enemy. The very nature of any communications mission gives them access to critical information about commanders, organizations, and locations of headquarters. This information, although gained casually on the job, is sensitive and must be protected. COMSEC must be a function of everyone who uses C-E equipment. It begins with command emphasis. FM 32-6 covers overall SIGSEC and contains detailed information on COMSEC measures and techniques.

b. ECCM techniques.

(1) ECCM are taken to protect against enemy attempts to detect, deceive, or destroy friendly communications. The first line of defense against REC is a well-trained and alert operator, because as mentioned earlier, many COMSEC techniques are equally ECCM techniques. To combat enemy REC efforts, operators must use ECCM techniques identified in OPSEC surveys and unit SOPs, or as outlined in table 9–2.

(2) Unit SOPS must include actions to be taken against jamming and deception. Specific techniques are described in TACSAT TMs. Prearranged plans and frequent training exercises are mandatory. Operators must follow SOPs to maintain or restore communications. Anti-jamming equipment may be available to some terminals. ECCM plans must consider possible up-link and down-link jamming. The jamming noise must be defeated by increases in transmit power or changes in link capacity.

(3) There are other ECCM actions that will lessen our vulnerability to an enemy REC effort.

(a) Prepare backup system-orderwire, messenger, and HF radio.

(b) Prepare to operate with the minimum amount of communications.

(c) Move CPs frequently.

(d) Use state-of-the-art equipment and apply authorized modifications to equipment.

(e) Report all known or suspected REC activities.

(f) Plan and train to counter an REC threat.

(g) Disperse communications equipment over a wide geographical area.

(4) FM 32-30 contains appendixes that cover ECCM checks, ECCM planning, and ECCM

Table 9-2. COMSEC measures and techniques

Physical Security	Crypto Security	Transmission Security	Emission Security
Facility approvals	Machine crypto	Emission control	Site surveys
Facility inspections	Non-machine crypto	Change of frequencies and call signs	Engineering
Materiel control system	Electronic crypto	Authentication codes and brevity lists	Inspections
Transportation security		Protective deception site masking	Studies
Storage security		Vary power directional antennas	Tests

training. It also covers EW reporting using the meaconing, intrusion, jamming, and interference (MIJI) report. AR 105-3 requires that all incidents of an electromagnetic nature that affect C-E opertions be reported. Unit SOP and other instructions must include the MIJI program.

c. Emission control.

(1) Emission control (EMCON) is both a COMSEC and ECCM technique and probably the best method to counter the enemy REC effort. Radio transmissions should be kept to the minimum required to accomplish the missions. Transmissions should be short. The enemy gains less information from a short transmission and it also limits the enemy's capability to locate the transmitter by RDF.

(2) EMCON can also be total or selective. sometimes, strict radio silence is necessary. The TACSAT Company commander may also designate certain nets as free nets and others as on order nets. Controls such as frequent changes in call signs and frequencies and relocation of emitters will tend to confuse the enemy. Commanders must teach their personnel to "think EMCON".

9-5. Electromagnetic compatibility

a. In an EW environment, we know that the enemy will intentionally try to interfere with Army communications. Self-inflicted unintentional interference is also possible. It may be caused by the Army's own transmitted signals, faulty electronic components, poorly insulated high power lines, noise producing equipment, and so forth. This type of interference is treated under the term "electromagnetic compatibility (EMC)." EMC is that desirable condition when all of our electronic and electrical equipment, such as radios, radars, generators, and vehicle ignition systems, operate without interfering with each other.

b. Terminal site planners and operators must be aware of EMC and its advantages. We do not want to assist the enemy in REC efforts. When planning the layout of the TACSAT Company CP or a terminal site, EMC must be considered. Operators experiencing interference must take every effort to determine if the interference is intentional or unintentional. The following are some typical common sense procedures to promote EMC:

(1) Know the technical operating characteristics of the equipment.

(2) Properly ground, operate, and maintain the equipment.

(3) Site antennas away from noise sources.

(4) Move noise-producing equipment out of transmission paths.

(5) Provide for adequate receiver-transmitter frequency separation.